CLAIMS

What is claimed is:

1. Apparatus for the secure installation and use of an information system having a plurality of nodes, where said plurality of nodes include at least one information appliance and at least one security console, comprising:

at least one data-carrying object containing security-related data; and

at least one object receptacle that comprises a portion of at least one of said nodes, a data-carrying object being inserted into said receptacle for reading-out the security-related data for indicating to the information system a desired security configuration.

2. Apparatus as in claim 1, wherein said data-carrying object stores the security-related data in a form that can be read-out by one of an electrical sensor, an optical sensor, or a magnetic sensor.

3. Apparatus as in claim 1, wherein said data-carrying object remains inserted in said receptacle for as long as the security configuration is desired to be in effect.

4. Apparatus as in claim 1, wherein said data-carrying object is temporarily made readable by said receptacle in order to initiate said security configuration.

5. Apparatus as in claim 1, wherein an information appliance has associated therewith at least one corresponding data-carrying object for inserting into said receptacle, wherein said receptacle has an output coupled

to said security console in an information system where the information appliance is intended to be used for indicating that the information appliance is one of a trusted information appliance or an untrusted information appliance.

6. Apparatus as in claim 1, wherein an information appliance is given access to information system resources, including information, by inserting a data-carrying object associated with said security console into said receptacle, said receptacle having an output that is coupled to said information appliance.

7. Apparatus as in claim 1, wherein each of said information appliance and said security console have associated therewith at least one corresponding data-carrying object, wherein a first receptacle has an output coupled to said security console in an information system where the information appliance is intended to be used for indicating, from security-related data contained on said data-carrying object associated with said information appliance, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second receptacle has an output coupled to said information appliance for indicating, from security-related data contained on said data-carrying object associated with said security console, that said security console is authorized to fulfil and originate requests for information appliance resources, including information.

8. Apparatus as in claim 1, wherein said data-carrying objects are obtained as a pair, wherein a first receptacle has an output coupled to said security console in an information system where the information appliance is intended to be used for indicating, from security-related

data contained on a first one of said pair of data-carrying objects, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second receptacle has an output coupled to said information appliance for indicating, from security-related data contained on a second one of said pair of data-carrying objects, that said security console is authorized to fulfil and originate requests for information appliance resources, including information.

9. Apparatus as in claim 1, wherein there are a plurality of said receptacles, and wherein an insertion of a data-carrying object into a first receptacle indicates different security-related information than inserting the data-carrying object into a second receptacle.

10. Apparatus as in claim 1, wherein said data-carrying objects are obtained as a pair, and wherein data-carrying objects in any given pair are the same shape, and no two data-carrying objects not in the same pair are the same shape.

11. Apparatus as in claim 1, wherein said data-carrying objects are obtained as a pair, and wherein data-carrying objects in any given pair are imprinted with a same visible identification information, and no two data-carrying objects not in the same pair are imprinted with the same visible identification information.

12. Apparatus as in claim 1, wherein said data-carrying objects are obtained as a pair, and wherein data-carrying objects in any given pair are fashioned so as to mechanically join together, and no two data-carrying objects not in the same pair will not or are unlikely to mechanically join together.

13. Apparatus as in claim 1, wherein data-carrying objects are obtained in groups of at least three, and where access to a resource, including information, is obtained by providing one subset of data-carrying objects from a group to a receptacle associated with a requestor of the resource, and a disjoint set of data-carrying objects from the same group is provided to the security console.

14. Apparatus as in claim 13, wherein identifications of all individual data-carrying objects in the group can be ascertained by viewing the security console, even if some subset of the data-carrying objects are provided to a receptacle associated with a requestor of the resource.

15. Apparatus as in claim 13, wherein a utilization of different disjoint subsets of the data-carrying objects in a group indicates different levels of trust to be granted to the requestor with respect to the resource.

16. Apparatus as in claim 13, wherein a utilization of different disjoint subsets of the data-carrying objects in a group indicates different levels of authorization to be granted to the requestor with respect to the resource.

17. Apparatus as in claim 13, wherein data-carrying objects in a particular group mechanically join together to form an assemblage, where the assemblage is adapted to be attached to a device through a single connection.

18. Apparatus as in claim 1, in which a newly-obtained information appliance is added to a group of authorized information appliances on behalf of a principal, by providing a data-carrying object representing the principal to a receptacle of the information appliance.

19. Apparatus as in claim 18, wherein said

data-carrying object representing the principal contains data which includes at least one secret known only to the principal.

20. Apparatus as in claim 19, wherein the secret known only to the principal comprises the private half of a public-private key pair associated with an asymmetric cryptosystem.

21. Apparatus as in claim 1, in which a certain principal, and at least one information appliance authorized to act on behalf of the principal, is granted a certain level of access to a certain resource by providing, to a receptacle associated with an information appliance representing the resource, a data-carrying object representing the principal.

22. Apparatus as in claim 21, wherein data contained in the data-carrying object representing the principal comprises the public half of a public-private key pair associated with an asymmetric cryptosystem.

23. Apparatus as in claim 22, in which the data-carrying object representing the principal comprises an image of the principal.

24. Apparatus as in claim 22, in which the data-carrying object representing the principal comprises a computer-readable data portion and an image of the principal.

25. Apparatus as in claim 24, further comprising a holder for holding the computer-readable data portion such that both the computer-readable data portion and the image are accessible.

26. A method for the secure installation and use of an information system having a plurality of nodes, where said plurality of nodes include at least one information appliance and at least one security console, comprising steps of:

providing at least one data-carrying object containing security-related data; and

inserting the data-carrying object into at least one object receptacle that comprises a portion of at least one of the nodes, the data-carrying object being inserted into the receptacle for reading-out the security-related data for indicating to the information system a desired security configuration.

27. A method as in claim 26, wherein the data-carrying object stores the security-related data in a form that can be read-out by one of an electrical sensor, an optical sensor, or a magnetic sensor.

28. A method as in claim 26, wherein the data-carrying object either remains inserted in the receptacle during the operation of the information system, or is temporarily inserted in or otherwise made readable by the receptacle either before or during the operation of the information system.

29. A method as in claim 26, wherein an information appliance has associated therewith at least one corresponding data-carrying object for inserting into the receptacle, wherein the receptacle has an output coupled to the security console in an information system where the information appliance is intended to be used for indicating that the information appliance is one of a trusted information appliance or an untrusted information

appliance.

30. A method as in claim 26, wherein an information appliance is given access to information system resources, including information, by inserting a data-carrying object associated with the security console into the receptacle, the receptacle having an output that is coupled to the information appliance.

31. A method as in claim 26, wherein each of the information appliance and the security console have associated therewith at least one corresponding data-carrying object, wherein a first receptacle has an output coupled to the security console in an information system where the information appliance is intended to be used for indicating, from security-related data contained on the data-carrying object associated with the information appliance, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second receptacle has an output coupled to the information appliance for indicating, from security-related data contained on the data-carrying object associated with the security console, that the security console is authorized to fulfil and originate requests for information appliance resources, including information.

32. A method as in claim 26, wherein the data-carrying objects are provided as a pair, wherein a first receptacle has an output coupled to the security console in an information system where the information appliance is intended to be used for indicating, from security-related data contained on a first one of the pair of data-carrying objects, that the information appliance is one that is authorized to fulfil and originate requests for information system resources, and wherein a second receptacle has an

output coupled to the information appliance for indicating, from security-related data contained on a second one of the pair of data-carrying objects, that the security console is authorized to fulfil and originate requests for information appliance resources, including information.

33. A method as in claim 26, wherein there are a plurality of the receptacles, and wherein an insertion of a data-carrying object into a first receptacle indicates different security-related information than inserting the data-carrying object into a second receptacle.

34. A method as in claim 26, wherein the data-carrying objects are provided as a pair, and wherein data-carrying objects in any given pair are the same shape, and no two data-carrying objects not in the same pair are the same shape.

35. A method as in claim 26, wherein the data-carrying objects are provided as a pair, and wherein data-carrying objects in any given pair are imprinted with a same visible identification information, and no two data-carrying objects not in the same pair are imprinted with the same visible identification information.

36. A method as in claim 26, wherein the data-carrying objects are provided as a pair, and wherein data-carrying objects in any given pair are fashioned so as to mechanically join together, and no two data-carrying objects not in the same pair will not or are unlikely to mechanically join together.

37. A method as in claim 26, wherein data-carrying objects are obtained in groups of at least three, and where access to a resource, including information, is obtained by providing one subset of data-carrying objects from a group

to a receptacle associated with a requestor of the resource, and a disjoint set of data-carrying objects from the same group is provided to the security console.

38. A method as in claim 37, wherein identifications of all individual data-carrying objects in the group can be ascertained by viewing the security console, even if some subset of the data-carrying objects are provided to a receptacle associated with a requestor of the resource.

39. A method as in claim 37, wherein a utilization of different disjoint subsets of the data-carrying objects in a group indicates different levels of trust to be granted to the requestor with respect to the resource.

40. A method as in claim 37, wherein a utilization of different disjoint subsets of the data-carrying objects in a group indicates different levels of authorization to be granted to the requestor with respect to the resource.

41. A method as in claim 37, wherein data-carrying objects in a particular group mechanically join together to form an assemblage, where the assemblage is adapted to be attached to a device through a single connection.

42. A method as in claim 26, in which access to the resource is denied unless every data-carrying object of the group is inserted into a receptacle.

43. A method as in claim 26, and further comprising a step of adding a newly-obtained information appliance to a group of authorized information appliances, on behalf of a principal, by inserting a data-carrying object representing the principal to a receptacle of the information appliance.

44. A method as in claim 43, wherein the data-carrying

object representing the principal contains data which includes at least one secret known only to the principal.

45. A method as in claim 44, wherein the secret known only to the principal comprises the private half of a public-private key pair associated with an asymmetric cryptosystem.

46. A method as in claim 26, in which a certain principal, and at least one information appliance authorized to act on behalf of the principal, is granted a certain level of access to a certain resource by inserting, to a receptacle associated with an information appliance representing the resource, a data-carrying object representing the principal.

47. A method as in claim 21, wherein data contained in the data-carrying object representing the principal comprises the public half of a public-private key pair associated with an asymmetric cryptosystem.

48. A method as in claim 47, in which the data-carrying object representing the principal comprises an image of the principal.

49. A method as in claim 47, in which the data-carrying object representing the principal comprises a computer-readable data portion and an image of the principal.

50. A method as in claim 49, further comprising a step of providing a holder for holding the computer-readable data portion such that both the computer-readable data portion and the image are accessible.

51. A computer program embodied on a computer-readable

medium for providing for the secure installation and use of an information system having a plurality of nodes, where said plurality of nodes include at least one information appliance and at least one security console, comprising code segments responsive to at least one data-carrying object containing security-related data that is inserted into at least one object receptacle that comprises a portion of at least one of the nodes, for reading-out the security-related data for determining, for the information system, a desired security configuration.